

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №1
ТЕМА «РАСЧЕТ ОБЪЕМА ОБОРУДОВАНИЯ ГИБКОГО КОММУТАТОРА
(SOFTSWITCH) СЕТИ NGN»

Цель занятия

Изучение методики и получение практических навыков проектирования гибкого коммутатора (softswitch), используемых в сетях связи следующего поколения NGN.

Литература

1. Росляков А.В. Сети следующего поколения. Часть II / Учебное пособие. – Самара, ПГАТИ, 2008, с. 123-147.
2. Семенов Ю.В. Проектирование сетей связи следующего поколения. – СПб., Наука и техника, 2005, с. 169-183.

Контрольные вопросы

1. Назначение и функции гибкого коммутатора (softswitch) в сети NGN.
2. Какие протоколы используются в гибком коммутаторе (softswitch) для управления сетью доступа?
3. Какие протоколы используются в гибком коммутаторе (softswitch) для управления транспортной сетью?
4. От чего зависит выбор производительности гибкого коммутатора (softswitch)?
5. Как рассчитывается нижний предел производительности гибкого коммутатора по обслуживанию сетей доступа?
6. Как рассчитывается нижний предел производительности гибкого коммутатора по обслуживанию транзитного уровня NGN?
7. Как определить необходимые интерфейсы для подключения гибкого коммутатора к пакетной сети?

Подготовка к занятию

1. Изучить указанную литературу.
2. Знать функции гибкого коммутатора (softswitch) в сети NGN.

Задание

В соответствии с индивидуальным заданием (см. табл. 1):

1. Изобразить проектируемую сеть NGN, обслуживаемую гибким коммутатором.
2. Рассчитать параметры гибкого коммутатора.

Содержание отчета

1. Таблица с исходными данными для проектирования гибкого коммутатора. Вариант индивидуального задания выбирается по последней цифре учебного шифра студента.
2. Схема подключения гибкого коммутатора к сети NGN с указанием используемых протоколов для управления сетью доступа и транспортной сетью.
3. Результаты расчетов оборудования гибкого коммутатора:
 - нижний предел производительности гибкого коммутатора для управления сетью доступа;
 - тип и количество интерфейсов подключения оборудования гибкого коммутатора к

пакетной сети для управления сетью доступа;

- суммарный минимальный полезный транспортный ресурс гибкого коммутатора SX, требуемый для обслуживания вызовов в транзитных коммутаторах;

- тип и количество интерфейсов подключения оборудования гибкого коммутатора к пакетной сети для управления транзитными коммутаторами.

Таблица 1 Индивидуальные задания

№	Исходный параметр	Варианты заданий									
		0	1	2	3	4	5	6	7	8	9
1.	Число абонентов ССОП	2000	2500	3000	3500	4000	4500	3000	2500	3500	2000
2.	Число абонентов ISDN-BRA	250	200	150	300	350	400	450	250	300	350
3.	Число сетей доступа с интерфейсом V.5/Число потоков E1 для подключения	2/5	3/3	5/4	0	3/5	2/1	6/3	4/4	3/6	0
4.	Число УПАТС, подключаемых к шлюзу /Число потоков PRI для подключения УПАТС	4/2	0	1/2	3/5	1/2	2/3	4/2	0	4/1	3/3
5.	Число абонентов с терминалами SIP/H.323/MGCP	500	450	600	250	350	550	300	400	200	450
6.	Поправочный коэффициент для ССОП	1,1	1,2	1,3	1,4	1,1	1,2	1,3	1,4	1,1	1,2
7.	Поправочный коэффициент для ISDN	1,3	1,5	1,6	1,2	1,4	1,3	1,2	1,1	1,5	1,4
8.	Поправочный коэффициент для V.5	1,2	1,3	1,5	1,1	1,2	1,4	1,5	1,3	1,2	1,1
9.	Поправочный коэффициент для УПАТС	1,5	1,1	1,1	1,3	1,3	1,5	1,1	1,2	1,3	1,3
10.	Поправочный коэффициент для пакетной сети	1,2	1,3	1,4	1,5	1,2	1,3	1,4	1,2	1,1	1,5
11.	Интенсивность вызовов, обслуживаемых одним каналом 64 кбит/с, вызовов/ЧНН	5	7	6	8	4	5	6	7	5	8
12.	Число потоков E1, используемых для подключения станции к транспортному шлюзу	2	3	4	5	2	3	4	2	3	5
13.	Число транспортных шлюзов, обслуживаемых гибким коммутатором	1	2	3	4	5	1	2	3	4	3

Методические указания

Уровень управления коммутацией и обслуживанием вызова в сети NGN

Задачей уровня управления коммутацией и передачей является управление установлением соединения в фрагменте сети NGN. Функция установления соединения реализуется на уровне элементов транспортной сети под внешним управлением оборудования гибкого коммутатора (softswitch). Исключением являются АТС с функциями MGC, которые сами выполняют коммутацию на уровне элемента транспортной сети.

Гибкий коммутатор должен осуществлять:

- обработку всех видов сигнализации, используемых в его домене;
- хранение и управление абонентскими данными пользователей, подключаемых к его домену непосредственно или через оборудование шлюзов доступа;
- взаимодействие с серверами приложений для предоставления расширенного списка услуг пользователям сети.

При установлении соединения оборудование гибкого коммутатора осуществляет сигнальный обмен с функциональными элементами уровня управления коммутацией. Такими элементами являются все шлюзы, терминальное оборудование сети (интегрированные устройства доступа (IAD), терминалы SIP и H.323), оборудование других гибких коммутаторов и АТС с функциями контроллера транспортных шлюзов (MGC). Для передачи информации сигнализации сети ТфОП через пакетную сеть используются специальные протоколы. Так, для передачи информации сигнализации ОКС№7, поступающей через сигнальные шлюзы от ТфОП к оборудованию гибкого коммутатора, используется протокол MxUA технологии SIGTRAN (в то же время в ряде реализаций гибкого коммутатора предусмотрен непосредственный ввод сигнализации ОКС№7).

На основании анализа принятой информации и решения о последующей маршрутизации вызова оборудование гибкого коммутатора, используя соответствующие протоколы, осуществляет сигнальный обмен по установлению соединения с сетевым элементом назначения и управляет с использованием протокола H.248 (для IP коммутации) или BICC (для ATM коммутации) установлением соединения для передачи пользовательской информации. При этом потоки пользовательской информации не проходят через гибкий коммутатор, а замыкаются на уровне транспортной сети.

В случае использования на сети нескольких гибких коммутаторов они взаимодействуют по межузловым протоколам (как правило, семейство SIP-T) и обеспечивают совместное управление установлением соединения.

Структура уровня управления сетями доступа NGN представлена на рис. 1.

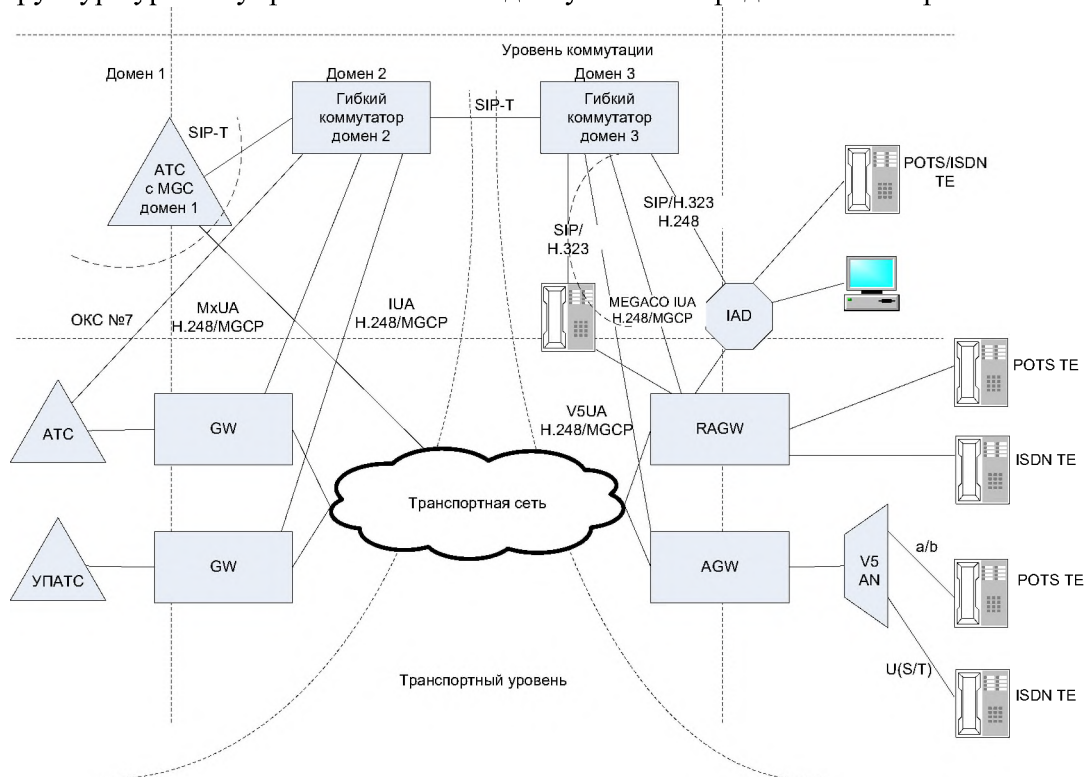


Рис. 1. Схема включения гибких коммутаторов для управления сетями доступа NGN

Терминальное оборудование пакетной сети взаимодействует с оборудованием гибкого коммутатора с использованием протоколов SIP и H.323. Пользовательская информация от

терминального оборудования поступает на уровень узлов доступа пакетной сети и далее маршрутизируется под управлением гибкого коммутатора.

Расчет производительности гибкого коммутатора

Основной задачей гибкого коммутатора при построении распределенного абонентского концентратора являются обработка сигнальной информации обслуживания вызова и управление установлением соединений. Емкостные параметры абонентской базы гибкого коммутатора должны позволять обслуживание всех абонентов различных типов, подключение которых планируется при построении абонентского концентратора. При этом для обслуживания вызовов могут использоваться различные протоколы сигнализации.

Введем следующие переменные:

P_{PSTN} — удельная интенсивность вызовов от абонентов, использующих доступ по аналоговой телефонной линии в ЧНН;

P_{ISDN} — удельная интенсивность вызовов от абонентов, использующих доступ по базовому доступу ISDN;

P_{V5} — удельная (приведенная к одному каналу интерфейса) интенсивность вызовов от абонентов, подключаемых к пакетной сети через сети доступа интерфейса V5;

P_{PBX} — удельная (приведенная к одному каналу интерфейса) интенсивность вызовов от УПАТС, подключаемых к пакетной сети;

P_{SHM} — удельная интенсивность вызовов от абонентов, использующих терминалы SIP, H.323, MGCP.

В соответствии с «Общими техническими требованиями к городским АТС» интенсивность вызовов равна:

$$P_{PSTN} = 5 \text{ выз/чнн}, \quad P_{ISDN} = 10 \text{ выз/чнн}, \quad P_{PBX} = 35 \text{ выз/чнн}.$$

Значение P_{SHM} можно принять равным P_{PSTN} . Значение P_{V5} можно принять равным P_{PBX} .

Тогда общая интенсивность вызовов, поступающих на гибкий коммутатор от источников всех типов, равна:

$$P_{CALL} = P_{PSTN} \cdot \left(\sum_{l=1}^L N_{l_PSTN} + \sum_{l=1}^L N_{l_SHM} \right) + P_{ISDN} \cdot \sum_{l=1}^L N_{l_ISDN} + P_{V5} \cdot \left(\sum_{l=1}^L \sum_{j=1}^J N_{j_V5} + \sum_{l=1}^L \sum_{k=1}^K N_{k_PX} \right) \quad (1)$$

где L — число шлюзов доступа, обслуживаемых гибким коммутатором.

Отметим, что удельная производительность коммутационного оборудования может отличаться в зависимости от типа обслуживаемого вызова, т.е. производительность при обслуживании, например, вызовов ССОП и ISDN, может быть разной.

В документации на коммутационное оборудование, как правило, указывается производительность для наиболее «простого» типа вызовов. В связи с чем при определении требований к производительности гибкого коммутатора можно ввести поправочные коэффициенты, которые характеризуют возможности системы по обслуживанию данного типа вызовов относительно «идеального» типа.

Например, если производительность системы для «идеальных» вызовов SIP равна 10 млн. выз/чнн, а для вызовов ССОП — 8 млн. выз/чнн, то интенсивность последних должна браться с коэффициентом 1,25.

Таким образом, нижний предел производительности гибкого коммутатора по обслуживанию потока вызовов с интенсивностью P_{CALL} может быть определен по формуле:

$$P_{SN} = k_{PSTN} \cdot P_{PSTN} \cdot N_{PSTN} + k_{ISDN} \cdot P_{ISDN} \cdot N_{ISDN} + k_{V5} \cdot P_{V5} \cdot N_{V5} + k_{PBX} \cdot P_{PBX} \cdot N_{PBX} + k_{SHM} \cdot P_{SHM} \cdot N_{SHM} \quad (2)$$

Следует отметить, что требования по производительности предполагают работу оборудования гибкого коммутатора в условиях перегрузки с показателями не ниже определяемых в рекомендации Q.543 для нагрузок классов В и С.

Расчет параметров интерфейсов подключения гибкого коммутатора к пакетной сети

Параметры интерфейса подключения гибкого коммутатора к пакетной сети определяются исходя из интенсивности обмена сигнальными сообщениями в процессе обслуживания вызовов.

Пусть:

L_{MEGACO} — средняя длина сообщения (в байтах) протокола MEGACO, используемого при передаче информации сигнализации по абонентским линиям;

N_{MEGACO} — среднее количество сообщений протокола MEGACO при обслуживании вызова;

L_{V5UA} — средняя длина сообщения протокола V5UA;

N_{V5UA} — среднее количество сообщений протокола V5UA при обслуживании вызова;

L_{IUA} — средняя длина сообщения протокола IUA;

N_{IUA} — среднее количество сообщений протокола IUA при обслуживании вызова;

L_{SH} — средняя длина сообщения протоколов SIP/H.323;

N_{SH} — среднее количество сообщений протоколов SIP/H.323 при обслуживании вызова;

L_{MGCP} — средняя длина сообщения протокола MGCP, используемого при управлении коммутацией на шлюзе;

N_{MGCP} — среднее количество сообщений протокола MGCP при обслуживании вызова.

Тогда:

$$V_{SX} = k_{sig} \cdot [(L_{MEGACO} \cdot N_{MEGACO} \cdot P_{PSTN} \cdot N_{PSTN} + L_{V5UA} \cdot N_{V5UA} \cdot P_{V5} \cdot N_{V5} + \\ + L_{IUA} \cdot N_{IUA} \cdot (P_{ISDN} \cdot N_{ISDN} + P_{PBX} \cdot N_{PBX}) + L_{SH} \cdot N_{SH} \cdot P_{SH} \cdot N_{SH} + \\ + L_{MGCP} \cdot N_{MGCP} \cdot (P_{PSTN} \cdot N_{PSTN} + P_{V5} \cdot N_{V5} + P_{ISDN} \cdot N_{ISDN} + P_{PBX} \cdot N_{PBX})] / 450 \quad (3)$$

где:

V_{SX} — минимальный полезный транспортный ресурс, в бит/с, которым гибкий коммутатор SX должен подключаться к пакетной сети, для обслуживания вызовов в сети доступа;

k_{sig} — коэффициент использования транспортного ресурса при передаче сигнальной нагрузки. По аналогии с расчетом сигнальной сети ОКС№7 примем значение $k_{sig} = 5$, что соответствует нагрузке в 0,2 Эрл;

1/450 — результат приведения размерностей «байт в час» к «бит в секунду» ($8/3600 = 1/450$).

Ориентировочно можно принять, что средняя длина всех сообщений равна 50 байтам, а среднее количество сообщений в процессе обслуживания вызова равно 10.

Емкостные параметры интерфейсов подключения оборудования гибкого коммутатора к пакетной сети определяются следующим выражением:

$$N_{INT} = \frac{V_{SX}}{V_{INT}} \quad (4)$$

где V_{INT} — полезный транспортный ресурс одного интерфейса.

Расчет оборудования гибкого коммутатора для управления транспортными коммутаторами

Основной задачей гибкого коммутатора при управлении транзитным уровнем коммутации в сети NGN является обработка сигнальной информации обслуживания вызова и управление установлением соединений. Требования к производительности гибкого коммутатора определяются интенсивностью вызовов, требующих обработки.

Интенсивность поступающих вызовов определяется интенсивностью вызовов, приходящейся на один канал 64 кбит/с первичного потока E1, а также числом потоков E1, используемых для подключения станции к транспортному шлюзу (рис. 2).

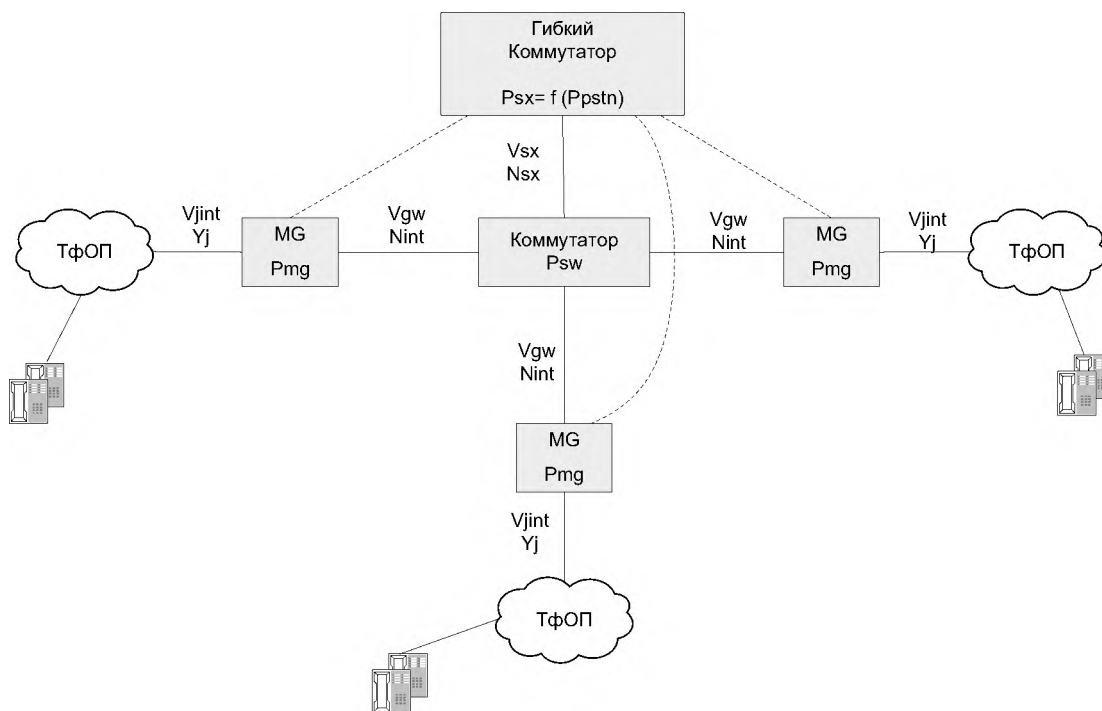


Рис. 2. Схема включения гибких коммутаторов для управления транзитным уровнем NGN

Пусть

P_{CH} — интенсивность вызовов, обслуживаемых одним каналом 64 кбит/с;

P_{GW} — интенсивность вызовов, обслуживаемых транспортным шлюзом.

Тогда интенсивность вызовов, поступающих на транспортный шлюз l , определяется формулой:

$$P_{l_GW} = N_{l_E1} \cdot 30 \cdot P_{CH}, \text{ выз/ЧНН} \quad (5)$$

Следовательно, интенсивность вызовов, поступающих на гибкий коммутатор, можно вычислить как

$$P_{SX} = \sum_{l=1}^L P_{l_GW} = 30 \cdot P_{CH} \cdot \sum_{l=1}^L N_{l_E1}, \text{ выз/ЧНН} \quad (6)$$

где L — число транспортных шлюзов, обслуживаемых гибким коммутатором.

Значение удельной интенсивности нагрузки определяется общими техническими требованиями к используемой опорной станции ОПС.

Требования по производительности предполагают работу оборудования гибкого коммутатора в условиях перегрузки с показателями не ниже определяемых в рекомендации Q.543 для нагрузок классов В и С.

Параметры интерфейса подключения гибкого коммутатора к пакетной сети определяются исходя из интенсивности обмена сигнальными сообщениями в процессе обслуживания

вызовов. При использовании гибкого коммутатора для организации распределенного транзитного коммутатора сообщения сигнализации ОКС№7 поступают на SX в формате сообщений протокола M2UA или M3UA, в зависимости от реализации.

Пусть:

L_{MXUA} — средняя длина сообщения (в байтах) протокола MxUA;

N_{MXUA} — среднее количество сообщений протокола MxUA при обслуживании вызова;

L_{MGCP} — средняя длина сообщения (в байтах) протокола MGCP, используемого для управления транспортным шлюзом;

N_{MGCP} — среднее количество сообщений протокола MGCP при обслуживании вызова.

Тогда транспортный ресурс SX, необходимый для передачи сообщений протокола MxUA, составляет:

$$V_{SX_MXUA} = k_{sig} \cdot L_{MXUA} \cdot N_{MXUA} \cdot P_{SX}, \text{ байт/ЧНН} \quad (7)$$

где k_{sig} — коэффициент использования ресурса.

Аналогично, транспортный ресурс гибкого коммутатора, необходимый для передачи сообщений протокола MGCP, составляет

$$V_{SX_MGCP} = k_{sig} \cdot L_{MGCP} \cdot N_{MGCP} \cdot P_{SX}, \text{ байт/ЧНН} \quad (8)$$

Суммарный минимальный полезный транспортный ресурс гибкого коммутатора SX, требуемый для обслуживания вызовов в структуре транзитного коммутатора, составляет

$$V_{SX} = V_{SX_MXUA} + V_{SX_MGCP}$$

После приведения размерностей получаем

$$V_{SX_MXUA} = k_{sig} \cdot P_{SX} \cdot (L_{MXUA} \cdot N_{MXUA} + L_{MGCP} \cdot N_{MGCP}) / 450, \text{ бит/с} \quad (9)$$

Также ориентировочно можно принять, что средняя длина всех сообщений равна 50 байтам, а среднее количество сообщений в процессе обслуживания вызова равно 10.

Емкостные параметры интерфейсов подключения оборудования гибкого коммутатора к пакетной сети для управления транзитными коммутаторами могут быть определены по формуле (4).

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №2

ТЕМА «ПОСТРОЕНИЕ СИГНАЛЬНЫХ ДИАГРАММ СОЕДИНЕНИЙ В СЕТИ NGN НА БАЗЕ ПРОТОКОЛА SIP»

Цель занятия

Изучение форматов сообщений протокола SIP и получение практических навыков построения сигнальных диаграмм и заполнения полей заголовков запросов и ответов.

Литература

1. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи /Учебник для ВУЗов. СПб.: БХВ-Петербург, 2010, с. 298-302.
2. Росляков А.В. Основы IP-телефонии / Учебное пособие. – М.: ИРИАС, 2007, с. 83-88.

Контрольные вопросы

1. Зачем нужен протокол SIP? Какие принципы положены в основу протокола SIP?
2. Какое место занимает протокол SIP в стеке протоколов TCP/IP?
3. С помощью какого протокола терминалы обмениваются информацией о своих функциональных возможностях?
4. Перечислите основные элементы SIP-сети, укажите их функции.
5. Из каких элементов состоит Агент пользователя? Когда они используются?
6. Перечислите типы серверов SIP-сети, укажите их функции
7. Привести пример SIP-сети. Описать на нем в общем виде процесс установления соединения между терминалами.
8. Какой тип адресации используется в протоколе SIP. Перечислить типы SIP-адресов, что значат их элементы?
9. Сообщения протокола SIP. Какой формат сообщений и их структура?
10. Назначение запросов и ответов протокола SIP.
11. Пояснить назначение основных заголовков сообщений.
12. Описать процесс установления соединения с участием сервера переадресации.
13. Описать процесс установления соединения с участием прокси-сервера.
14. В чем разница двух сценариев?
15. Какое минимальное число сообщений необходимо для установления соединения?

Подготовка к занятию

1. Изучить указанную литературу.
2. Знать основные принципы протокола SIP.

Задание

Исходные данные:

1. Соединение между пользователями А и В в сети NGN на базе протокола SIP устанавливается через прокси-серверы, обслуживающих этих пользователей. Прокси-серверы знают текущее местоположение пользователей.
2. Пользователи А и В в сети NGN на базе протокола SIP характеризуются данными, приведенными в табл. 1.
3. Адреса (имена) прокси-серверов пользователей А и В задать самостоятельно в том же домене, что и пользователь.

Таблица 1. Исходные данные для задания. Вариант индивидуального задания выбирается по предпоследней цифре учебного шифра студента.

Номер варианта	0	1	2	3	4	5	6	7	8	9
Имя пользователя А	User	Operat	Guest	Privacy	Client	Managr	People	Chief	Boss	Clerk
Отображаемое имя пользователя А	Vladimir	Olga	Peter	Ivan	Lena	David	Sofia	Sasha	Nina	Sergei
Домен пользователя А	prim.ru	darts.ru	doc.com	ant.org	guk.ru	mtusi.ru	force.int	astan.kz	mins.bu	kiev.ua
IP-адрес пользователя А	192.168.0.1	196.14.1.12	207.12.2.51	212.1.0.3	198.1.1.3	195.2.3.11	211.11.1.1	195.0.2.4	199.1.0.32	193.24.1.0
Номер предыдущей последовательности команд	25486	3648	31975	593173	2132456	553547	4358	23787	5867	67867
Имя пользователя В	Guest	Privacy	User	Operat	People	Boss	Client	Managr	Clerk	Chief
Отображаемое имя пользователя В	Olga	Peter	Lena	Vladimir	Sofia	Nina	Sergei	David	Sasha	Ivan
Домен пользователя В	darts.ru	doc.com	prim.ru	mtusi.ru	ant.org	doc.com	guk.ru	guk.ru	astan.kz	docum.com
IP-адрес пользователя В	192.130.1.0	193.23.1.2	223.2.0.1	202.14.3.91	197.12.1.3	194.26.2.11	191.3.12.3	211.0.2.1	196.35.0.3	194.32.5.1
Исход вызова	Успешное соединение, отбой пользов А	Неуспешное соединение, пользов В занят	Успешное соединение, отбой пользов А	Неуспешное соединение, прокси - сервер В не имеет возможности обслужить запрос	Успешное соединение, отбой пользов. А	Неуспешное соединение, в прокси - сервере В не реализованы функции	Успешное соединение, отбой пользов А	Неуспешное соединение, запрос не понят прокси-сервером В из-за наличия в нем синтаксических ошибок	Неуспешное соединение, прокси-сервер В перегружен	Неуспешное соединение, прокси-сервер В отказался обслуживать запрос

Необходимо:

1. Изобразить стрелочную диаграмму установления успешного соединения и его разрушения между пользователями А и В в сети на базе протокола SIP с указанием используемых запросов и ответов протокола SIP.
2. Для каждого запроса и ответа заполнить поле заголовков.

Содержание отчета

1. Стрелочная диаграмма установления успешного соединения и его разрушения между пользователями А и В в сети NGN на базе протокола SIP.
2. Заполненные поля заголовков всех использованных в соединении запросов и ответов протокола SIP.

Методические указания

Сценарии установления соединений

Сценарий установления соединения через сервер переадресации

Вызывающему пользователю требуется вызвать другого пользователя. Он передает запрос INVITE (1) на известный ему адрес сервера переадресации и на порт 5060, используемый по умолчанию (рис. 1).

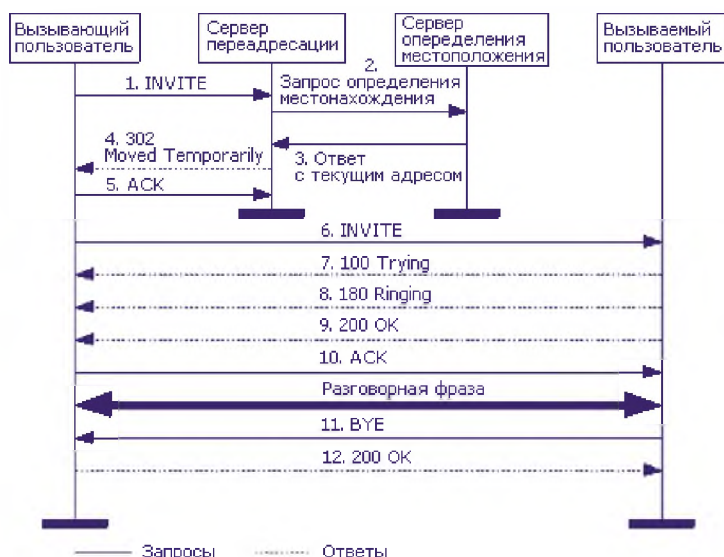


Рис. 1 Сценарий установления соединения через сервер переадресации

В запросе вызывающий пользователь указывает адрес вызываемого пользователя. Сервер переадресации запрашивает текущий адрес нужного пользователя у сервера определения местоположения (2), который сообщает ему этот адрес (3). Сервер переадресации в своем ответе 302 Moved temporarily передает вызывающей стороне текущий адрес вызываемого пользователя (4), или сообщает список зарегистрированных адресов вызываемого пользователя, предлагая вызывающему самому выбрать один из них. Вызывающая сторона подтверждает прием ответа 302 передачей сообщения ACK (5).

Теперь вызывающая сторона может связаться с вызываемой стороной. Для этого она передает новый запрос INVITE (6). В теле сообщения INVITE указываются данные о функциональных возможностях вызывающей стороны в формате протокола SDP. Вызываемая сторона принимает запрос INVITE и начинает его обработку, о чем сообщает ответом 100 Trying (7) встречному оборудованию для перезапуска его таймеров.

После завершения обработки поступившего запроса оборудование вызываемой стороны сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ 180 Ringing (8). После приема вызываемым пользователем входящего вызова встречной стороне передается сообщение 200 OK (9), в котором содержатся данные о функциональных возможностях вызываемого терминала в формате протокола SDP. Терминал вызывающего пользователя подтверждает прием ответа запросом ACK (10). На этом фаза установления соединения заканчивается, и начинается разговорная фаза.

По завершении разговорной фазы любая из сторон передает запрос BYE (11), который подтверждается ответом 200 OK (12).

Если пользователь А знает о текущем местоположении пользователя В, то он не обращается к серверу переадресации и серверу определения местоположения.

Сценарий установления соединения через прокси-сервер

В этом случае действия (1), (2), (3) такие же, как и при использовании сервера переадресации. После выяснения адреса (на сервере определения местоположения) прокси-сервер пользователя А передает по этому адресу запрос INVITE (4) (рис. 2). Вызываемый пользователь В оповещается акустическим или визуальным сигналом о том, что его вызывают (5); он поднимает трубку, и ответ 200 ОК отправляется к прокси-серверу (6). Прокси-сервер переправляет этот ответ вызвавшему пользователю А (7), последний подтверждает правильность приема, передавая запрос ACK (8), который переправляется к вызванному пользователю В (9). Соединение установлено, идет разговор.

Вызванный пользователь В кладет трубку, передается запрос BYE (8), прием которого подтверждается ответом 200 ОК (9).

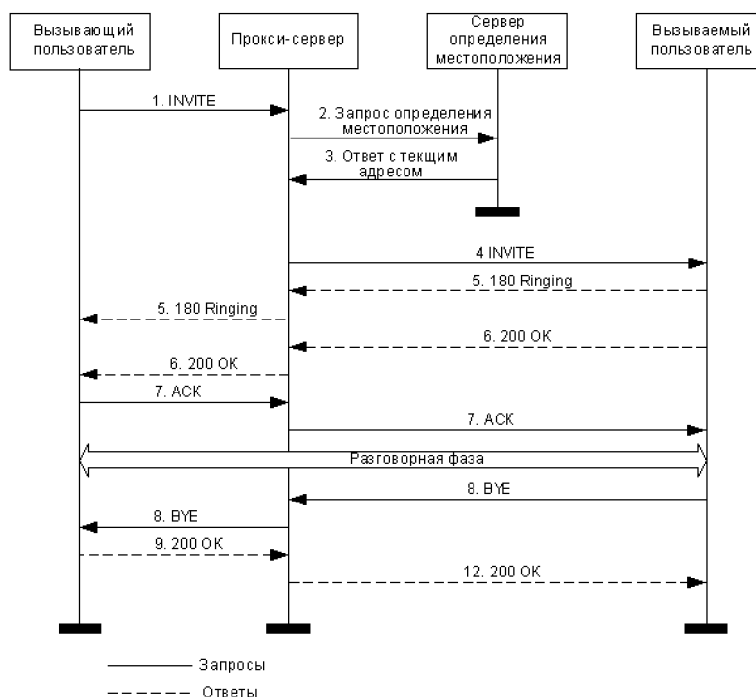


Рис. 2. Сценарий установления соединения через прокси-сервер

Если прокси-сервер пользователя А знает о текущем местоположении пользователя В, то он не обращается к серверу определения местоположения.

Создание запроса протокола SIP

Сообщения протокола SIP (запросы и ответы), представляют собой последовательности текстовых строк, закодированных в соответствии с документом RFC 2279. Структура и синтаксис сообщений SIP идентичны используемым в протоколе HTTP (рис. 3).



Рис. 3. Структура сообщений протокола SIP

Запрос протокола SIP, составленный клиентом агента пользователя UAC (User Agent Client), должен *обязательно* включать:

- *стартовую строку* Request-Line;
- *шесть полей заголовков*: To, From, CSeq, Call-ID, Max-Forwards и Via.

Стартовая строка Request-Line состоит из названия типа запроса, адрес запроса Request-URI и номера версии протокола, разделённых пробелом (рис. 4). Request-Line заканчивается символами возврата каретки и перевода строки (CRLF). Оба символа, вместе или по одиночке, не должны встречаться в других частях строки.

Тип запроса	Пробел	Request-URI	Пробел	Версия протокола	CRLF
-------------	--------	-------------	--------	------------------	------

Рис 4. Структура строки Request-Line

В базовой рекомендации IETF RFC 3261 определено *6 типов запросов*: REGISTER - для регистрации контактной информации, INVITE, ACK и CANCEL - для установление сессий, BYE - для завершения сессий и OPTIONS - для запроса информации о функциональных возможностях сервера. В настоящее время число запросов в протоколе SIP увеличено до 14. Сервер определяет тип принятого запроса по названию, указанному в стартовой строке.

Поле Request-URI - это SIP URI, указывающий на пользователя или сервис, к которому адресован запрос. Исходное значение поля Request-URI сообщения устанавливается таким же, как URI в поле To. При использовании предустановленного маршрута рекомендуется задавать один URI, соответствующий исходящему прокси-серверу. Поле Request-URI не должно содержать пробелов и управляющих символов, а также быть заключённым в угловые скобки «< >».

И запросы, и ответы содержат действующую версию SIP-протокола. Приложения, посылающие SIP-сообщения, должны в поле SIP-Version указывать SIP/2.0.

Пример стартовой строки:

ACK sip:alex@psuti.ru SIP/2.0

Ниже будет рассмотрено формирование заголовков SIP-запросов при работе UAC вне диалога. Примерами запросов, отсылаемых вне диалога, является запрос INVITE, устанавливающий сессию, и запрос OPTIONS для запроса информации о функциональных возможностях. SIP-запросы при работе UAC в режиме диалога должны содержать специальный параметр, определяющий конкретный терминал вызываемого пользователя.

Формирование заголовка To

Поле заголовка To устанавливает желаемого логического получателя запроса - публичный адрес получателя (address-of-record) или ресурс, на который отправляется запрос. Значение заголовка может как быть, так и не быть конечным получателем запроса. Поле To должно содержать SIP или SIPS URI. Схема SIPS означает, что ресурсы достижимы только при условии обеспечения безопасности (например, с помощью протокола TLS). Поле To позволяет также отображать имя пользователя (display name).

Обычно поле заголовка To заполняется через интерфейс пользователя вручную или с использованием адресной книги. Зачастую пользователь не вводит адреса полностью, а вместо этого вводит строку букв или цифр (например, «alex»); агент пользователя UA (User Agent) сам решает, как интерпретировать эту строку. Использование строки ввода для формирования пользовательской части SIP-адреса (user part) предполагает, что UA желает определить имя домена, находящееся по правую сторону от «@» SIP URI (например, sip: alex@psuti.ru).

Запросы вне диалога не должны содержать параметра «tag» в поле To. Параметр «tag» в заголовке To определяет конкретный терминал вызываемого пользователя (например, домашний, рабочий или сотовый телефон) из терминалов, зарегистрированных под одним SIP адресом. «Tag» заголовка To в совокупности с «tag» заголовка From и значением поля Call-ID

идентифицирует диалог между двумя его участниками. Поскольку диалог не был установлен, «tag» в запросе отсутствует.

Пример поля заголовка To:

To: Alex <sip:alex@psuti.ru>

Формирование заголовка From

Поле заголовка From содержит логический идентификатор инициатора сообщения, как правило, публичный адрес вызывающего пользователя. Так же, как поле To, оно содержит URI и, опционально, отображаемое имя (display name), что удобно для вызываемого пользователя. Заголовок используется SIP-элементами для того, чтобы определить правила обработки, применимые к запросу (например, автоматическое отклонение вызова). Важно, чтобы URI в заголовке From не содержал IP-адреса хоста, с которым работает UA, так как это не логические имена.

Заголовок From предусматривает присутствие отображаемого имени (display name). UAC должен использовать отображаемое имя «Anonymous», если идентификационная информация пользователя (identity) неизвестна.

Обычно, поле заголовка From запросов, которые создаёт UA, заполняется на основании значения, предварительно определённого пользователем или администратором локального домена пользователя. Если конкретный UA используется несколькими пользователями, он может иметь переключаемые профили, которые содержат URI, соответствующий конкретным пользователям. Получатели запросов могут аутентифицировать инициатора запроса для того, чтобы убедиться, что они те, кого представляют заголовки From их запросов.

Поле From должно содержать новый параметр «tag», созданный клиентом UA. Этот параметр содержит произвольную буквенно-цифровую строку, которая добавляется к URI UAC. Она используется для идентификации сессии.

Примеры поля заголовка From:

From: "Bob" <sips:bob@biloxi.com> ;tag=a48s

From: sip: +12125551212@phone2net.com;tag=887s

From: Anonymous <sip:c8oqz84zk7z@privacy.org>;tag=hyh8

Формирование заголовка Call-ID

Заголовок Call-ID – это уникальный идентификатор, объединяющий группу сообщений. Он должен совпадать для всех запросов и ответов, отправляемых любым из двух UA в процессе диалога. При создании нового диалога, заголовок Call-ID должен быть выбран UAC как уникальный идентификатор. Все SIP-агенты пользователя должны иметь средства, чтобы гарантировать, что Call-ID, созданный ими, не будет случайно генерирован другим UA.

При генерации значений Call-ID рекомендуется использовать случайные криптографические идентификаторы (по RFC 1750), их использование обеспечивает некоторую защиту от взлома сессий и уменьшает вероятность возникновения коллизий Call-ID. Значения заголовка Call-ID чувствительны к регистру и должны сравниваться побайтно.

Когда запросы отправляются повторно после получения ответа с кодом ошибки, требующего коррекции запроса, (например, запрос на предоставление отклика аутентификации), эти повторные запросы не рассматриваются как новые и они передаются со старым значением заголовка Call-ID.

Пример поля заголовка Call-ID:

Call-ID: f81d4fae-7dec-11d0-a765-00a0c91e6bf6@psuti.ru

Формирование заголовка CSeq

Поле заголовка CSeq (Sequence Command) служит средством для идентификации и упорядочивания транзакций в диалоге. Поле заголовка CSeq содержит порядковый номер и тип запроса. Для запросов вне диалога, кроме REGISTER, значение порядкового номера может быть произвольным. Величина порядкового номера выражается 32-разрядным целым числом и должна быть меньше, чем 2^{31} . Клиент может выбирать любой механизм для создания значений заголовка CSeq.

Пример поля заголовка CSeq:
CSeq: 456 INVITE

Формирование заголовка Max-Forwards

Заголовок Max-Forwards используется в любом типе SIP-запросов, чтобы ограничить число серверов или шлюзов, через которые проходит запрос на пути к месту назначения. Значение заголовка должно быть целым числом в пределах от 0 до 255, отражающим оставшееся количество пересылок, которое разрешено для сообщения. Это число уменьшается каждым сервером на единицу, который пересылает запрос дальше. В качестве первоначального значения рекомендуется брать 70. Величина выбрана достаточно большой, чтобы гарантировать, что запрос не будет отброшен сетью SIP при отсутствии петель, но и не слишком большой, чтобы не загружать ресурсы прокси-сервера при возникновении петли. Меньшие величины рекомендуется использовать с осторожностью и только в сетях, где агенту пользователя известна топология сети.

Пример поля заголовка Max-Forwards:
Max-Forwards:6

Формирование заголовка Via

Поле заголовка Via указывает один из узлов, используемых для проведения транзакции и идентифицирует местоположение (location), куда должен быть отправлен ответ. SIP элемент, добавляет собственное значение заголовка Via только после выбора следующего узла, которому будет передан запрос.

Когда UAC создает запрос, он должен вставить в него поле Via. Также необходимо указать название протокола – SIP, и его версию - 2.0. Поле заголовка Via должно содержать параметр «branch». Этот параметр используется для идентификации транзакции, созданной данным запросом. Он используется и клиентом, и сервером.

Значение параметра «branch» должно быть уникальным для всех запросов, отправляемых UA. Исключение составляют запрос CANCEL и запрос ACK на ответы, отличные от класса 2xx. Запрос CANCEL будет иметь то же значение параметра «branch», что и запрос, который он отменяет. Запрос ACK на ответ, отличный от класса 2xx также будет иметь тот же параметр «branch», что и INVITE, ответ на который он подтверждает. Уникальность этого параметра облегчает его использование в качестве идентификатора транзакции. Параметр «branch», вставляемый элементом сети SIP, должен всегда начинаться с "z9hG4bK". Эти семь символов, называемых «magic cookie» («волшебное печенье»), используют для того, чтобы серверы, получившие запрос, могли определить, что идентификатор транзакции уникален в мировом масштабе. Содержимое куки, как правило, не значимо для получателя и не интерпретируется до тех пор, пока получатель не вернёт куки обратно отправителю. В реальной жизни куки можно сравнить с номерком в гардеробе: номерок не имеет собственной ценности, но он позволяет получить взамен правильное пальто.

Пример заголовка Via:
Via: SIP/2.0/UDP 12.26.17.91:5060; branch=z9hG4bK3af7.0a6e92f4
v: SIP/2.0/UDP server10.itep.com

Укажем назначение некоторых других заголовков, часто встречающихся в сообщениях SIP:

В заголовок **Record route (Хранимый маршрут)** прокси-сервер вписывает свой адрес – SIP URL, – если хочет, чтобы последующие запросы прошли через него.

Заголовок **Content Type (Тип тела сообщения)** определяет формат описания сеанса связи. Само описание сеанса, например, в формате протокола SDP, включается в тело сообщения.

Заголовок **Content Length (Длина тела сообщения)** указывает в десятичном виде размер тела сообщения в байтах.

Следует обратить внимание на то, что запросы и ответы на них могут включать в себя лишь определенный набор заголовков (табл. 1). Здесь буква «М» означает обязательное присутствие заголовка в сообщении, буква «О» – необязательное присутствие, буква «F» запрещает присутствие заголовка. * – поле необходимо только в случае, когда тело сообщения содержит какую-либо информацию, т.е. не является пустым.

Таблица 1 Связь заголовков с запросами и ответами протокола SIPv2.0

Название заголовка	Место использования заголовка	ACK	BYE	CAN	INV	OPT	REG
Accept	Заголовок в запросах	F	F	F	O	O	O
Accept	Заголовок в ответе 415	F	F	F	O	O	O
Accept-Encoding	Заголовок в запросах	F	F	F	O	O	O
Accept-Encoding	Заголовок в ответе 415	F	F	F	O	O	O
Accept-Language	Заголовок в запросах	F	O	O	O	O	O
Accept-Language	Заголовок в ответе 415	F	O	O	O	O	O
Allow	Заголовок в ответе 200	F	F	F	F	M	F
Allow	Заголовок в ответе 405	O	O	O	O	O	O
Authorization	Заголовок в запросах	O	O	O	O	O	O
Call-ID	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Contact	Заголовок в запросах	O	F	F	O	O	O
Contact	Заголовок в ответах 1xx	F	F	F	O	O	F
Contact	Заголовок в ответах 2xx	F	F	F	O	O	O
Contact	Заголовок в ответах 3xx	F	O	F	O	O	O
Contact	Заголовок в ответе 485	F	O	F	O	O	O
Content-Encoding	Заголовки содержания	O	F	F	O	O	O
Content-Length	Заголовки содержания	O	F	F	O	O	O
Content-Type	Заголовки содержания	*	F	F	*	*	*
Cseq	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Date	Заголовок в ответах	O	O	O	O	O	O
Encryption	Заголовок в ответах	O	O	O	O	O	O
Expires	Заголовок в ответах	F	F	F	O	F	O
From	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Hide	Заголовок в запросах	O	O	O	O	O	O
Max-Forwards	Заголовок в запросах	O	O	O	O	O	O
Organization	Общий заголовок	F	F	F	O	O	O
Proxy-Authenticate	Заголовок в ответе 407	O	O	O	O	O	O
Proxy-Authorization	Заголовок в запросах	O	O	O	O	O	O
Proxy-Require	Заголовок в запросах	O	O	O	O	O	O
Priority	Заголовок в запросах	F	F	F	O	F	F
Require	Заголовок в запросах	O	O	O	O	O	O
Retry-After	Заголовок в запросах	F	F	F	F	F	O
Retry-After	Заголовок в ответах 404, 480, 486, 503, 600 и 603	O	O	O	O	O	O
Response-Key	Заголовок в запросах	F	O	O	O	O	O
Record-Route	Заголовок в запросах	O	O	O	O	O	O
Record-Route	Заголовок в ответах 2xx	O	O	O	O	O	O
Route	Заголовок в запросах	O	O	O	O	O	O
Server	Заголовок в ответах	O	O	O	O	O	O
Subject	Заголовок в запросах	F	F	F	O	F	F
Timestamp	Общий заголовок	O	O	O	O	O	O
To	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Unsupported	Заголовок в ответе 420	O	O	O	O	O	O
User-Agent	Общий заголовок	O	O	O	O	O	O
Via	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Warning	Заголовок в ответах	O	O	O	O	O	O
WWW-Authenticate	Заголовок в ответе 401	O	O	O	O	O	O

Создание ответа протокола SIP

Характерное отличие SIP-ответов от запросов – это наличие строки состояния Status-Line, в состав которой входят версия протокола и код ответа (Status-Code) со связанной с ним текстовой расшифровкой (Reason-Phrase), разделённые пробелом. Символы возврата каретки (CR) и перевода строки (LF) могут использоваться только совместно в завершающей строку последовательности CRLF.

Версия протокола	Пробел	Код ответа	Пробел	Расшифровка ответа	CRLF
---------------------	--------	---------------	--------	-----------------------	------

Код ответа – это целое трёхзначное число, отражающее результат обработки запроса сервером. Расшифровка ответа (Reason-Phrase) дает краткое описание кода ответа и предназначена для визуального восприятия пользователем в отличие от кода ответа (Status-Code), который служит для оповещения технических устройств. К формулировке расшифровки ответа (Reason-Phrase) не предъявляются жестких требований.

Определено шесть типов ответов, несущих разную функциональную нагрузку. Тип ответа кодируется трехзначным числом. Самой важной является первая цифра, которая определяет класс ответа, остальные две цифры лишь дополняют первую. В некоторых случаях оборудование даже может не знать все коды ответов, но оно обязательно должно интерпретировать первую цифру ответа.

Все ответы делятся на две группы: *информационные и финальные*.

Информационные ответы кодируются трехзначным числом, начинающимся с единицы, **1xx** и показывают, что запрос находится в стадии обработки. Информационные ответы показывают, что запрос находится в стадии обработки. Некоторые информационные ответы, например, 100 Trying, предназначены для установки на ноль таймеров, которые запускаются в оборудовании, передавшем запрос. Если к моменту срабатывания таймера ответ на запрос не получен, то считается, что этот запрос потерян и может (по усмотрению производителя) быть передан повторно. Один из распространенных ответов - 180 Ringing; по назначению он идентичен сигналу «Контроль посылки вызова» в ТфОП и означает, что вызываемый пользователь получает сигнал о входящем вызове.

Финальные ответы кодируются трехзначными числами, начинающимися с цифр **2, 3, 4, 5 и 6**. Они означают завершение обработки запроса и содержат, когда это нужно, результат обработки запроса.

Ответы 2xx означают, что запрос был успешно обработан. В настоящее время из всех ответов типа 2xx определен лишь два - 200 OK и 202 Accepted.

Значение ответа 200 OK зависит от того, на какой запрос он отвечает:

- ответ 200 OK на запрос INVITE означает, что вызываемое оборудование согласно на участие в сеансе связи; в теле ответа указываются функциональные возможности этого оборудования;
- ответ 200 OK на запрос BYE означает завершение сеанса связи, в теле ответа никакой информации не содержится;
- ответ 200 OK на запрос CANCEL означает отмену поиска, в теле ответа никакой информации не содержится;
- ответ 200 OK на запрос REGISTER означает, что регистрация прошла успешно;
- ответ 200 OK на запрос OPTIONS служит для передачи сведений о функциональных возможностях оборудования, эти сведения содержатся в теле ответа.

Ответ 202 Accepted означает, что запрос был принят для обработки, но обработка еще не завершена.

Ответы 3xx информируют оборудование вызывающего пользователя о новом местоположении вызываемого пользователя или переносят другую информацию, которая может быть использована для нового вызова:

- в ответе *300 Multiple Choices* указывается несколько SIP-адресов, по которым можно найти вызываемого пользователя, и вызывающему пользователю предлагается выбрать один из них;

- ответ *301 Moved Permanently* означает, что вызываемый пользователь больше не находится по адресу, указанному в запросе, и направлять запросы нужно на адрес, указанный в поле Contact;

- ответ *302 Moved Temporary* означает, что пользователь временно (промежуток времени может быть указан в поле Expires) находится по другому адресу, который указывается в поле Contact.

Ответы 4xx информируют о том, что в запросе обнаружена ошибка. После получения такого ответа пользователь не должен передавать тот же самый запрос без его модификации:

- ответ *400 Bad Request* означает, что запрос не понят из-за наличия в нем синтаксических ошибок;

- ответ *401 Unauthorized* означает, что запрос требует проведения процедуры аутентификации пользователя. Существуют разные варианты аутентификации, и в ответе может быть указано, какой из них использовать в данном случае;

- ответ *403 Forbidden* означает, что сервер понял запрос, но отказался его обслуживать. Повторный запрос посылать не следует. Причины могут быть разными, например, запросы с этого адреса не обслуживаются и т.д.;

- ответ *485 Ambiguous* означает, что адрес в запросе не определяет вызываемого пользователя однозначно;

- ответ *486 Busy Here* означает, что вызываемый пользователь в настоящий момент не может принять входящий вызов по данному адресу. Ответ не исключает возможности связаться с пользователем по другому адресу или, к примеру, оставить сообщение в речевом почтовом ящике.

Ответы 5xx информируют о том, что запрос не может быть обработан из-за отказа сервера:

- ответ *500 Server Internal Error* означает, что сервер не имеет возможности обслужить запрос из-за внутренней ошибки. Клиент может попытаться повторно послать запрос через некоторое время;

- ответ *501 Not Implemented* означает, что в сервере не реализованы функции, необходимые для обслуживания этого запроса. Ответ передается, например в том случае, когда сервер не может распознать тип запроса;

- ответ *502 Bad Gateway* информирует о том, что сервер, функционирующий в качестве шлюза или прокси-сервера, принял некорректный ответ от сервера, к которому он направил запрос;

- ответ *503 Service Unavailable* говорит о том, что сервер не может в данный момент обслужить вызов вследствие перегрузки или проведения технического обслуживания.

Ответы 6xx информируют о том, что соединение с вызываемым пользователем установить невозможно:

- ответ *600 Busy Everywhere* сообщает, что вызываемый пользователь занят и не может принять вызов в данный момент ни по одному из имеющихся у него адресов. Ответ может указывать время, подходящее для вызова пользователя;

- ответ *603 Decline* означает, что вызываемый пользователь не может или не желает принять входящий вызов. В ответе может быть указано подходящее для вызова время;

- ответ *604 Does Not Exist Anywhere* означает, что вызываемого пользователя не существует.

Пример ответа 200 OK:

SIP/2.0 200 OK

Via: SIP/2.0/UDP kton.bell-tel.com

From: A. Bell <sip:a.g.bell@bell-tel.com>

To: <sip:watson@bell-tel.com>;

Call-ID: 3298420296@kton.bell-tel.com

Cseq: 1 INVITE

Content-Type: application/sdp

Content-Length: ...

v=0

o=watson 4858949 4858949 IN IP4 192.1.2.3

t=3149329600 0

SIP=IN IP4 boston.bell-tel.com

m=audio 5004 RTP/AVP 0 3

a=rtpmap:0 PCMU/8000

a=rtpmap:3 GSM/8000

В ответе пользователя Watson на запрос Bell сообщается, что он может принимать аудиоинформацию на порт 5004, понимает кодеки PCMU, GSM. Поля From, To, Via, Call-ID взяты из запроса. Поле Cseq показывает, что это – ответ на INVITE с Cseq: 1.

Пример запросов и ответов SIP при установлении соединения с использованием двух прокси-серверов

1. Пользователь U1 посылает запрос INVITE прокси-серверу P1 для связи с пользователем callee в домене domain.com:

INVITE sip:callee@domain.com SIP/2.0

Contact: sip:caller@u1.example.com

2. Прокси-сервер P1 не отвечает за домен domain.com, он обращается к серверу DNS и получает от него доменное имя получателя. Он также добавляет в запрос заголовок Record-Route:

INVITE sip:callee@domain.com SIP/2.0

Contact: sip:caller@u1.example.com

Record-Route: <sip:p1.example.com;lr>

Параметр `lr` в SIP заголовке `Record-Route` указывает, что SIP прокси-сервер является маршрутизатором со свободным выбором маршрутов.

2. Прокси-сервер P2 получает запрос INVITE. Так как он отвечает за домен `domain.com`, то он может реализовать услугу и обработать запрашиваемый адрес `Request-URI`. Он также добавляет в заголовок строку `Record-Route` со своим именем и определяет новый `Request-URI`, по которому следует передать запрос:

```
INVITE sip:callee@u2.domain.com SIP/2.0
Contact: sip:caller@u1.example.com
Record-Route: <sip:p2.domain.com;lr>
Record-Route: <sip:p1.example.com;lr>
```

5. Вызываемый пользователь U2 с именем `callee` и адресом `u2.domain.com` принимает запрос INVITE и высылает ответ 200 OK:

```
SIP/2.0 200 OK
Contact: sip:callee@u2.domain.com
Record-Route: <sip:p2.domain.com;lr>
Record-Route: <sip:p1.example.com;lr>
```

6. Вызываемый пользователь U2 также устанавливает состояние диалога с удаленным адресом URI `sip:caller@u1.example.com` и его маршрут включает:
(`<sip:p2.domain.com;lr>`, `<sip:p1.example.com;lr>`)

7. Далее ответ маршрутируется к прокси-серверу P2, а затем к пользователю U1. Пользователь, U1 устанавливает состояние диалога с удаленным адресом URI `sip:callee@u2.domain.com` и его маршрут включает:

(`<sip:p1.example.com;lr>`, `<sip:p2.domain.com;lr>`)

8. Так как все компоненты маршрута содержат параметр `lr`, пользователь передает запрос BYE следующего вида:

```
BYE sip:callee@u2.domain.com SIP/2.0
Route: <sip:p1.example.com;lr>, <sip:p2.domain.com;lr>
```

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №3

ТЕМА «РАЗРАБОТКА СХЕМ ВЗАИМОДЕЙСТВИЯ ТРАДИЦИОННЫХ ТЕЛЕФОННЫХ СЕТЕЙ И СЕТЕЙ NGN»

Цель занятия

Изучение процессов установления телефонных соединений с совместным использованием протоколов сигнализации ISUP и SIP и получение практических навыков построения сигнальных диаграмм взаимодействия телефонных сетей и сетей NGN.

Литература

1. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи /Учебник для ВУЗов. СПб.: БХВ-Петербург, 2010, с. 298-302.

2. Росляков А.В. Система общеканальной сигнализации ОКС№7 / Учебное пособие. – М.: ИРИАС, 2007, с. 83-88.

Контрольные вопросы

1. В каких узлах сети происходит преобразование сообщений протоколов ISUP и SIP при установлении и разрушении пользовательских соединений? Какие функции они выполняют в сетях SIP и ОКС№7?
2. Какие базовые сообщения передаются в сети сигнализации ОКС№7 (ISUP) при установлении и разрушении телефонного соединения?
3. Какие базовые запросы и ответы передаются в сети SIP при установлении и разрушении речевого соединения?
4. Каким образом передается информация о причине неуспешного соединения в сети на базе протокола SIP?
5. Каким образом передается информация о причине неуспешного соединения в сети сигнализации ОКС№7 (ISUP)?

Подготовка к занятию

1. Изучить указанную литературу.
2. Знать основные принципы протоколов SIP и ISUP.

Задание

1. Изобразить схему организации связи между исходящим и входящим терминалами через транзитную сеть в соответствии с индивидуальным заданием, указанным в таблице 1.
2. Указать назначение сетевых узлов, используемых при организации соединений между терминалами разных сетей.
3. Определить:
 - тип используемых протоколов сигнализации на каждом участке взаимодействия сетей;
 - тип используемых протоколов для передачи речевой информации между терминалами на каждом участке соединения;
 - вид передаваемой информации на каждом участке взаимодействия сетей.
4. Изобразить стрелочную диаграмму обмена сигнальными сообщениями между сетевыми узлами, используемыми при организации соединения между терминалами разных сетей.
5. Указать, какую основную информацию переносит каждое сигнальное сообщение.

Содержание отчета

3. Стрелочная диаграмма установления соединения между пользователями А и В с указанием:
 - типов сетевых узлов;
 - типов используемых протоколов сигнализации на каждом участке взаимодействия сетей;
 - типов используемых протоколов для передачи речевой информации между терминалами на каждом участке соединения;
 - типов сообщений ISUP и SIP и их информационного содержания.

Таблица 1. Исходные данные для задания. Вариант индивидуального задания выбирается по последней цифре учебного шифра студента.

№ варианта	Тип исходящего терминала	Исходящая сеть	Тип транзитной сети	Тип входящего терминала	Входящая сеть	Исход соединения
1	Аналоговый	ТфОП	NGN	Аналоговый	ТфОП	Успешное, отбой абонента Б
2	Аналоговый	NGN	ТфОП	Аналоговый	ТфОП	Неуспешное, занятость абонента Б
3	SIP	NGN	NGN	Аналоговый	ТфОП	Неуспешное, неответ абонента Б
4	SIP	NGN	NGN	Аналоговый	ТфОП	Успешное, отбой абонента А
5	SIP	NGN	ТфОП	SIP	NGN	Неуспешное, неправильный номер абонента Б
6	SIP	NGN	ТфОП	Аналоговый	NGN	Успешное, отбой абонента Б
7	Аналоговый	NGN	NGN	Аналоговый	ТфОП	Неуспешный, абонент Б занят
8	Аналоговый	ТфОП	ТфОП	SIP	NGN	Неуспешное, неответ абонента Б
9	Аналоговый	NGN	NGN	SIP	NGN	Неуспешный, абонент Б занят
0	Аналоговый	NGN	NGN	Аналоговый	ТфОП	Неуспешное, неответ абонента Б

Методические указания

Общие положения

Далее представлены процедуры, которые может использовать контроллер медиашлюзов MGC (выполняющий функцию шлюза сигнализации SGW) при взаимодействии сетей ТфОП (работающей с системой сигнализации OKC№7 и подсистемой ISUP) и NGN (использующей протокол сигнализации SIP), путем иллюстрации соответствий между протоколами SIP и ISUP на уровне сообщений и уровне параметров. Основное внимание уделено трансляции сообщений ISUP в сообщения SIP и отображению параметров ISUP в заголовках SIP. Для вызовов ISUP, которые проходят через сеть SIP, целью трансляции является разрешить элементам SIP, таким как прокси-серверы (которые обычно не могут обрабатывать сообщения ISUP), принимать решения по маршрутизации на основе такого критерия ISUP, как номер вызываемой стороны. Отображение между сигнальными сообщениями протоколов ISUP и SIP описывается с использованием диаграмм потоков вызова. На приведенных ниже диаграммах вся сигнализация (SIP, ISUP) к и от MGC выполняется сигнальным шлюзом, а оперирование медиа-информацией (проектирование речевого канала, освобождение канала) выполняется медиашлюзом MG под управлением контроллера MGC. Для упрощения они показаны на рисунках одним узлом, обозначенным как «MGC/MG».

Соединения SIP → ISUP

Установление успешного соединения

1. Когда пользователь SIP желает инициировать сеанс связи с пользователем ТфОП, узел SIP выдает запрос INVITE, шлюз посылает на него ответ 100 Trying.

2. При приеме запроса INVITE шлюз отображает его в сообщение ISUP «Начальное адресное сообщение» (IAM) и посылает его в сеть ОКС№7.
3. Удаленный узел ISUP информирует, что абонент свободен и адрес достаточен для установления соединения путем посылки сообщения ISUP «Адрес полный» (ACM).
4. Получив сообщение ACM, шлюз отображает код события (event code) в промежуточный ответ SIP 180 Ringing (Посылка вызова) и посылает его на узел SIP. Пользователю SIP передается тональный сигнал «Контроль посылки вызова».
5. Когда пользователь ТфОП ответит, шлюзу посылается сообщение ISUP «Ответ» (ANM).
6. Приняв сообщение ANM, шлюз посылает сообщение 200 OK к узлу SIP.
7. Узел SIP, получив финальный ответ 200 OK, посылает сообщение ACK для подтверждения.

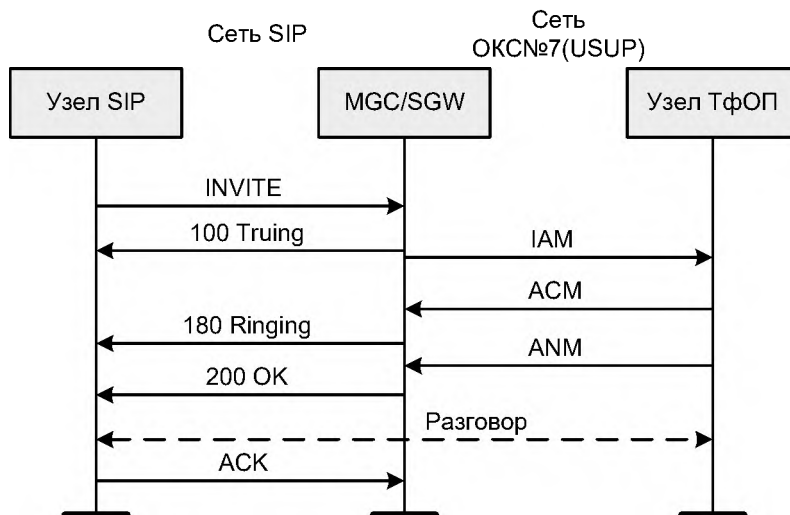


Рис. 1. Установление успешного соединения

Невозможность установления соединения в сети ISUP

1. Когда пользователь SIP инициирует сеанс связи с пользователем ТфОП, узел SIP генерирует запрос INVITE.
2. Приняв запрос INVITE, шлюз отображает его в сообщение IAM и посылает его в сеть ISUP.
3. Т.к. удаленный узел ISUP не может установить соединение, он посылает сообщение REL.
4. Шлюз освобождает канал и подтверждает, что он свободен для дальнейшего использования посылкой сообщения RLC.
5. Шлюз транслирует код причины из сообщения REL в ответ SIP об ошибке 4xx и передает его на узел SIP.
6. Узел SIP посылает ACK для подтверждения приема финального ответа INVITE.

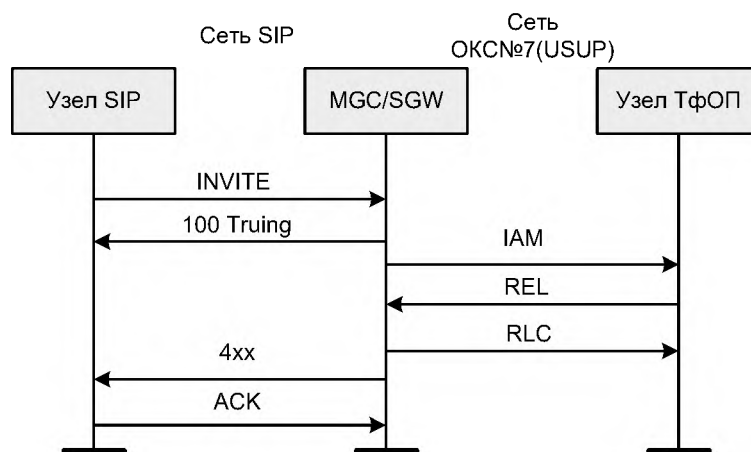


Рис. 2 - Невозможность установления соединения в сети ISUP

Отбой вызова на стороне SIP до ответа абонента ТфОП

1. Когда пользователь SIP инициирует сеанс связи с пользователем ТфОП, узел SIP генерирует запрос INVITE.
2. Приняв запрос INVITE, шлюз отображает его в сообщение IAM и посылает его в сеть ISUP.
3. Удаленный узел ISUP информирует, что абонент свободен и адрес достаточен для установления соединения путем посылки сообщения ACM.
4. Код параметра «called party status» (статус вызываемой стороны) из сообщения ACM отображается в промежуточный ответ SIP 180.
5. Для завершения вызова до ответа абонента узел SIP посылает запрос CANCEL.
6. Запрос CANCEL подтверждается ответом 200 OK.
7. Получив запрос CANCEL, шлюз посылает ISUP сообщение REL для завершения вызова.
8. Шлюз посылает ответ 478 «Call Cancelled» (Вызов отменен) на узел SIP для завершения транзакции INVITE.
9. Получив сообщение REL, удаленный узел ISUP отвечает сообщением RLC.
10. Получив ответ 487, узел SIP подтверждает прием сообщением ACK.

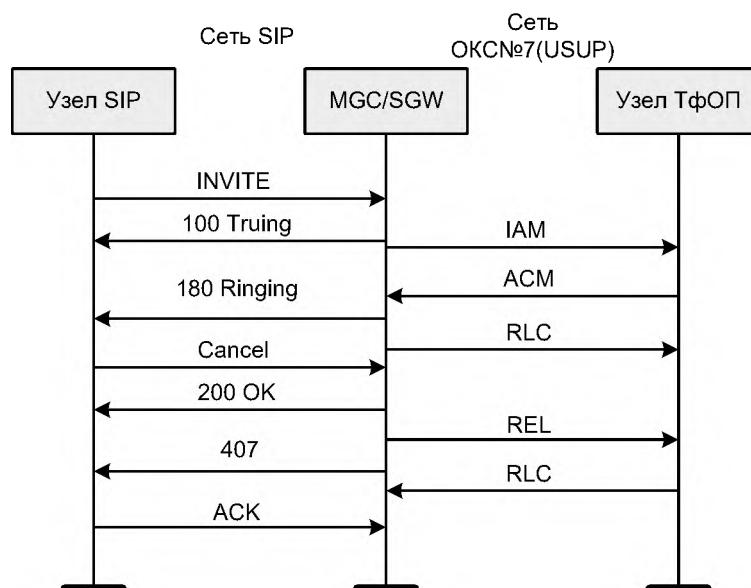


Рис. 3 - Отбой вызова со стороны сети SIP

Соединения ISUP→SIP

Установление успешного соединения

1. Когда абоненту ТфОП требуется начать установку сеанса к абоненту SIP, ТфОП генерирует сообщение IAM в направлении шлюза.

2. При приеме сообщения IAM шлюз генерирует сообщение INVITE и посылает его соответствующему узлу SIP.

3. Если происходит событие, обозначающее, что адресная информация вызова является достаточной, то узел SIP генерирует предварительный ответ 180 Ringing или больший.

4. При приеме предварительного ответа 180 Ringing или большего шлюз генерирует сообщение ACM. Если ответ был не 180 Ringing, то в сообщении ACM значение параметра «called party status» («статус вызываемой стороны») будет «no indication» («не указано»).

5. Когда узел SIP ответит на вызов, он посылает сообщение 200 OK.

6. При приеме сообщения 200 OK шлюз посылает сообщение ANM в направлении узла ISUP.

7. Для подтверждения приема окончательного ответа на INVITE шлюз посылает сообщение ACK узлу SIP.

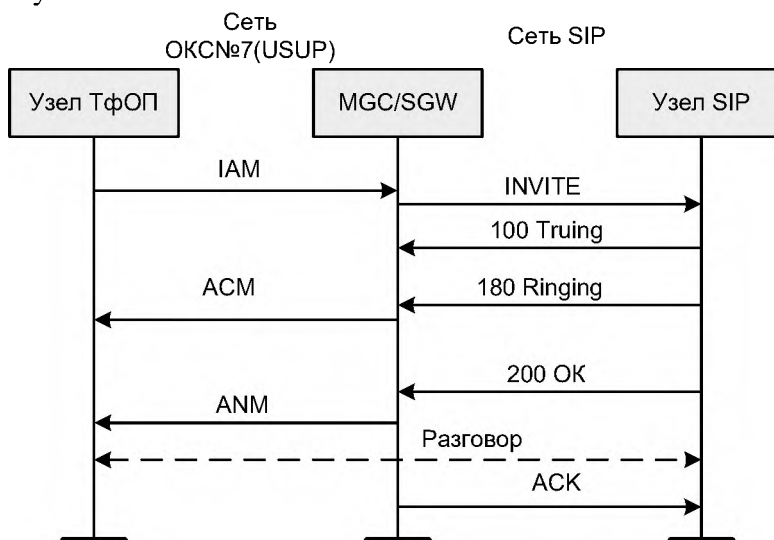


Рис. 4 Установление успешного соединения

Установление неуспешного соединения в сети SIP

1. Когда абоненту ТфОП требуется начать установку сеанса к абоненту SIP, ТфОП генерирует сообщение IAM в направлении шлюза.

2. При приеме сообщения IAM шлюз генерирует сообщение INVITE и посылает его соответствующему узлу SIP на основе анализа номера вызываемого абонента.

3. Узел SIP указывает на состояние ошибки ответом с кодом 400 или большим.

4. Для подтверждения приема окончательного ответа на INVITE шлюз посылает сообщение ACK узлу SIP.

5. Сообщение REL ISUP с соответствующим кодом причины генерируется из узла SIP.

6. Удаленный узел ISUP подтверждает прием сообщения REL сообщением RLC.

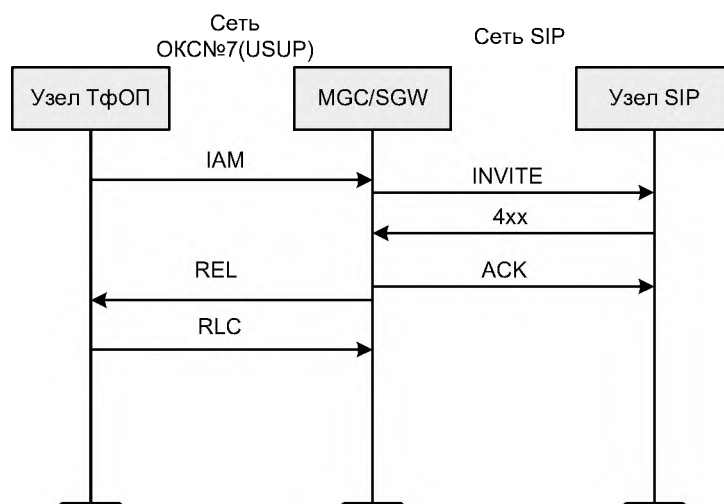


Рис. 5 - Установление неуспешного соединения в сети SIP

Перенаправление вызова в сети SIP

1. Когда абоненту ТфОП требуется начать установку сеанса к абоненту SIP, ТфОП генерирует сообщение IAM в направлении шлюза.

2. При приеме сообщения IAM шлюз генерирует сообщение INVITE и посылает его соответствующему узлу SIP на основе анализа номера вызываемого абонента.

3. Узел SIP посылкой ответа 3xx указывает, что ресурс, к которому пользователь пытается установить контакт, расположен в другом месте. Предполагается, что контактный URL указывает действительный URL, который доступен VoIP SIP-вызову.

4. Шлюз подтверждает прием окончательного ответа на INVITE, передавая сообщение ACK узлу SIP.

5. Шлюз посылает принятое сообщение INVITE по адресу, указанному в поле контакт сообщения 3xx.

6. Когда происходит событие, говорящее о том, что вызов имеет достаточную адресную информацию, узел SIP генерирует предварительный ответ 180 Ringing или больший.

7. При приеме предварительного ответа 180 Ringing или большего шлюз генерирует сообщение ACM с кодом события.

8. Когда узел SIP отвечает на вызов, он посылает сообщение 200 OK.

9. При приеме сообщения 200 OK шлюз посылает сообщение ANM в направлении узла ISUP.

10. Для подтверждения приема окончательного ответа на INVITE шлюз посылает сообщение ACK узлу SIP.

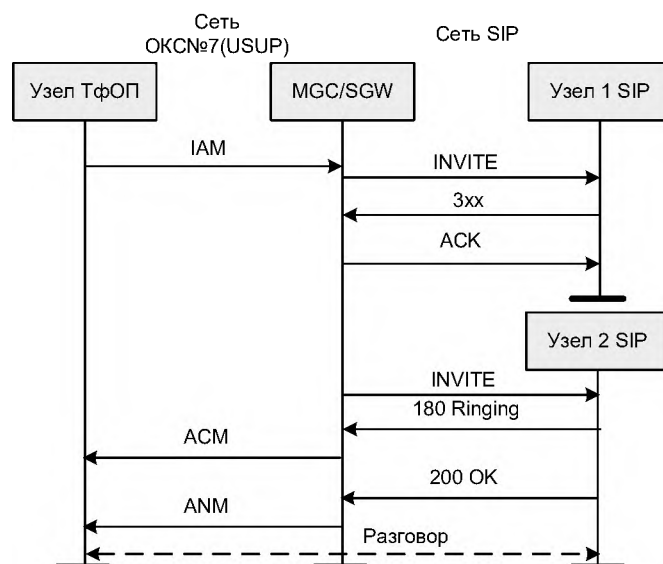


Рис. 6 - Перенаправление вызова в сети SIP

Разъединение соединения со стороны ISUP

1. Когда абоненту ТфОП требуется начать установку сеанса к абоненту SIP, ТфОП генерирует сообщение IAM в направлении шлюза.

2. При приеме сообщения IAM шлюз генерирует сообщение INVITE и посылает его соответствующему узлу SIP на основе анализа номера вызываемого абонента.

3. Когда происходит событие, говорящее о том, что вызов имеет достаточную адресную информацию, узел SIP генерирует предварительный ответ 180 Ringing или больший.

4. При приеме предварительного ответа 180 Ringing или большего шлюз генерирует сообщение ACM с кодом события.

5. Если вызывающий абонент положит трубку раньше, чем поступит ответ на вызов от узла SIP, то будет генерироваться сообщение REL.

6. Шлюз освобождает линию ТфОП и посылкой RLC показывает, что она доступна для нового использования.

7. При приеме сообщения REL до заключительного ответа на INVITE шлюз посылает сообщение CANCEL в направлении узла SIP.

8. При приеме сообщения CANCEL узел SIP посылает ответ 200.

9. Удаленный узел SIP посылает ответ 487 Call Cancelled («Запрос закончен») для завершения транзакции INVITE.

10. Для подтверждения приема окончательного ответа на INVITE шлюз посылает сообщение ACK узлу SIP.

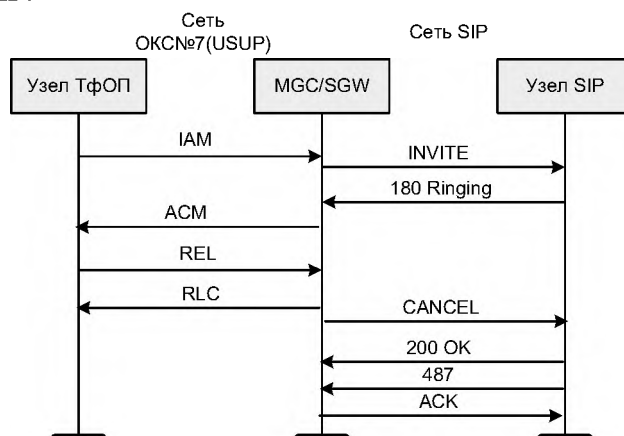


Рис. 7 - Разъединение соединения со стороны ISUP